10/688,026

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月１７日

出願番号
Application Number: 特願２００２－３０２４３９

[ST. 10/C]: ［ＪＰ２００２－３０２４３９］

出願人
Applicant(s): 株式会社日立製作所

２００３年１０月１５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０８４５７６

【書類名】　特許願

【整理番号】　K02010221A

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　荒井　正人

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　甲斐　賢

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】ポリシー設定支援ツール

【特許請求の範囲】

【請求項１】

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、前記ポリシー情報の作成に要する作業負荷を軽減するためのポリシー設定支援ツールであって、

当該ポリシー設定支援ツールは、アクセス主体となるサブジェクトの種類毎に用意した情報と、アクセス対象となるオブジェクトの種類毎に用意した情報から、適切なポリシーを作成するものであり、

前記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、

前記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報からなり、

更に前記ポリシー設定支援ツールは、前記サブジェクトの動作を監視して前記アクセスログ情報に記録するためのアクセス監視部と、前記サンプル情報と前記インストール情報とを照合して差分を検出する差分検出部と、前記サンプル情報と前記関連付け情報と前記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による更なるポリシーの修正および保存をするためのユーザインタフェース部とから構成されることを特徴とするポリシー設定支援ツール。

【請求項２】

請求項１記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールの利用者は、前記ユーザインタフェース部を通じて、前記サンプル情報と、前記関連付け情報と、前記アクセスログ情報とから、

１つ以上の情報を用いてポリシーの原案を作成し、当該ポリシー原案を元に必要に応じて更に修正を加え、修正後のポリシーを保存することで、前記ポリシー情報を設定することを特徴とするポリシー設定支援ツール。

【請求項３】

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、前記ポリシー情報の維持に要する作業負荷を軽減するためのポリシー設定支援ツールであって、

アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、当該差分検出部による検出結果からポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による目視確認および前記ポリシーの更新処理をするためのユーザインタフェース部とから構成されることを特徴とするポリシー設定支援ツール。

【請求項４】

請求項３記載のポリシー設定支援ツールであって、

前記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、前記ユーザインタフェース部を通じて利用者向けに表示し、

前記ポリシー設定支援ツールの利用者は、前記ユーザインタフェース部を通じて表示される前記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば前記ユーザインタフェース部を通じて必要な修正を加えた上で、前記ポリシー情報を保存することを特徴とするポリシー設定支援ツール。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータシステムが管理する情報資産に対するアクセスを、所定のポリシーに基づいてコントロールするアクセス制御システムにおいて、上記ポリシーの作成および維持に要する作業負荷を軽減する場合に好適なポリシー設

定支援ツールに関する。

【０００２】

【従来の技術】

一般のコンピュータシステムでは、マルチユーザ・マルチタスクＯＳが備えるユーザ認証機構と、該認証結果に基づいたアクセス制御機構を用いて情報その他コンピュータ資源の保護を実現しているケースが多い。具体的には、上記ＯＳが実装された情報処理装置を利用する際に、ユーザは必ず自己のユーザＩＤとパスワードを入力し、認証を受ける。

【０００３】

上記情報処理装置が管理する全てのファイル各々には、ファイル読み出しや書き込み等のアクセスタイプ毎に、ユーザＩＤとグループＩＤを用いてアクセス可能なユーザを定義したアクセスコントロールリスト（以下、ポリシーと称す）がセキュリティ属性情報として割り当てられている。

【０００４】

ユーザがアプリケーションプログラムを介してファイルへアクセスした場合、上記ＯＳは、アクセス要求元となるユーザのＩＤ及び該ユーザが所属するグループのＩＤを、アクセス対象となるファイルやディレクトリに割り当てられたポリシーと照合し、当該リストに上記ユーザが含まれている場合に限りアクセスを許可するといった制御を行う。

【０００５】

また、アクセス要求元の情報として、上記ユーザＩＤやグループＩＤだけでなく、例えばアクセス手段となるプログラムの識別子まで確認すれば、より厳密なアクセス制御が可能となる。

【０００６】

このようなアクセス制御の方法は、例えば特許文献１に開示されている。ただし、不正アクセスを防止するには、本来の利用目的であるサービス提供や業務遂行の上で必要最小限のアクセスのみ許可されるよう、上記ポリシーを設定しておくことが重要である。

【０００７】

その他、特許文献２には、セキュリティポリシーの作成に要する時間を短縮するために、複数の雛形のポリシーから自己に見合ったものを選択し、修正しながらポリシーを作成する方法が開示されている。

【０００８】

【特許文献１】

特開２００１－３３７８６４号公報

【特許文献２】

特開２００２－１０８８１８号公報

【０００９】

【発明が解決しようとする課題】

先に述べたように、情報資産を安全に利用するためには、当該情報への必要最小限のアクセスのみ許可するようにポリシーを定義することが重要である。

【００１０】

しかし、ユーザＩＤやグループＩＤだけでなく、アクセス手段となるプログラムの識別子まで組み合わせてポリシーを定義することは、厳密なアクセス権チェックができる代わりに、そのポリシー作成に手間がかかる。例えば、どのようなデータにアクセスするかといったソフトウェアの仕様を知らなければ、適切なポリシーは設定できない。

【００１１】

ソフトウェアが複数のプログラムから構成されている場合は、特に難しいと言える。上記特許文献２に記載されている方法を用いても、雛形のポリシーを自己に見合ったものに修正するのは全て利用者自身であるため、ソフトウェアの仕様を知らなければ、どこをどのように修正すべきか判断できないケースも発生し得る。

【００１２】

また、プログラムアップデートによるプログラムファイル自体の変更が発生したり、ユーザやグループの登録内容に変更が発生したり、更には情報資産であるファイルやディレクトリが、削除・移動・名称書き換え等により変更されることで、現在のポリシーの記述と一致しなくなれば、適切なアクセス制御ができなく

なるという問題もある。

【００１３】

そこで、本発明の第一の目的は、利用するソフトウェアの仕様を知らなくても、コンピュータの利用目的を果たす上で適切なファイルアクセスのみを許可するようにポリシーを設定可能な、ポリシー設定支援ツールを提供することにある。

【００１４】

本発明の第二の目的は、アクセス主体となるユーザやプログラムの情報の他、アクセス対象となるファイルやディレクトリ等に変更があった場合でも、簡易な操作により関連するポリシーの設定内容を更新可能な、ポリシー設定支援ツールを提供することにある。

【００１５】

【課題を解決するための手段】

上記第一の目的を達成するために、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の作成に要する作業負荷を軽減するためのポリシー設定支援ツールであって、当該ポリシー設定支援ツールは、アクセス主体となるサブジェクトの種類毎に用意した情報と、アクセス対象となるオブジェクトの種類毎に用意した情報から、適切なポリシーを作成するものであり、上記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、上記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報からなり、更に上記ポリシー設定支援ツールは、上記サブジェクトの動作を監視して上記アクセスログ情報に記録するためのアクセス監視部と、上記サンプル情報と上記インストール情報とを照合して差分を検出する差分検出部と、上記サンプル情報と上記関連付け情報と上記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による更なるポリシー

の修正および保存をするためのユーザインタフェース部とから構成されることを特徴としている。

【００１６】

上記ポリシー設定支援ツールによれば、例えばソフトウェアの種類毎にサンプルとなるポリシーが提供され、且つ対象のコンピュータシステムに適合したポリシーの原案まで自動的に作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

【００１７】

また、本発明は、上記ポリシー設定支援ツールにおいて、当該ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて、上記サンプル情報と、上記関連付け情報と、上記アクセスログ情報とから、１つ以上の情報を用いてポリシーの原案を作成し、当該ポリシー原案を元に必要に応じて更に修正を加え、修正後のポリシーを保存することで、上記ポリシー情報を設定することを特徴としている。

【００１８】

これにより、上記サンプルとなるポリシーが用意されていない場合でも、上記関連付け情報やアクセスログ情報からポリシーの原案が作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

【００１９】

また、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の維持に要する作業負荷を軽減するためのポリシー設定支援ツールであって、アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、当該差分検出部による検出結果の表示処理と、利用者による目視確認および上記ポリシーの更新処理をするためのユーザインタフェース部とから構成されることを特徴としている。

【００２０】

これにより、アクセス主体となるサブジェクトの情報や、アクセス対象となるオブジェクトに変更があった場合でも、更新すべき項目を自動的に検出して表示できるので、簡易な操作で関連するポリシーの更新が可能となる。

【００２１】

また、本発明は、上記ポリシー設定支援ツールにおいて、上記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、上記ユーザインタフェース部を通じて利用者向けに表示し、上記ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて表示される上記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば上記ユーザインタフェース部を通じて必要な修正を加えた上で、上記ポリシー情報を保存することを特徴としている。

【００２２】

これにより、利用者は上記ユーザインタフェース部を通じて、差分情報の確認と、ポリシーの修正および保存まで、ポリシーの更新に必要な処理を全て行うことができる。

【００２３】

また、定期的な差分検出処理も可能とすることで、利用者が自ら上記差分検出部に対して要求を出さなくても差分情報を取得できるようになるため、無効なポリシー記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

【００２４】

【発明の実施の形態】

以下、図を用いて本発明の実施の一形態を説明する。

【００２５】

図１は、本実施形態のポリシー設定支援ツールの一構成例である。ポリシー設定支援ツール１００は、ユーザインタフェース部１０１と、ポリシー生成部１０２、アクセス監視部１０３、差分検出部１０４、インストール情報１０５、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８から構成される。

【００２６】

１１０はアクセス制御部であり、サブジェクト１１１からオブジェクト１１２へのアクセスの可否をポリシー情報１２０の記述内容に従って判定し、ポリシーに合致したアクセスのみ許可し、ポリシー違反のアクセスであれば上記サブジェクト１１１にエラーを返すといった処理を行う。

【００２７】

このようなアクセス制御は、一般的なオペレーティングシステム（ＯＳ）でも標準で備えているが、それらが参照するポリシー情報の多くは、オブジェクトへアクセス可能なサブジェクトを、ユーザやグループの識別子を用いて指定したものである。

【００２８】

これに対して、本実施形態のポリシー設定支援ツールが扱うポリシー情報とは、ユーザやグループの識別子だけでなく、少なくともアクセス手段として用いるプログラムの情報を組み合わせてアクセス権を指定したものである。

【００２９】

なお、サブジェクト情報１１３は、本実施例においてはインストールされているプログラムファイル群や、登録されているユーザ・グループに関する情報を指す。

【００３０】

上記ポリシー設定支援ツール１００は、上記各種情報１０５～１０７や、上記サブジェクト１１１からオブジェクト１１２へのアクセスを記録したアクセスログ１０８を利用しながらポリシー情報１２０の設定作業を容易にするものである。また、上記サブジェクト情報１１３を参照しながら、ポリシーの更新作業を容易にするものでもある。

【００３１】

図２は、上記ポリシー設定支援ツール１００を利用するために必要なシステムの一例を示したものである。図２において、情報処理装置２００は、中央演算処理装置ＣＰＵ２０１ａと、主記憶２０２ａ、外部記憶装置２０３ａ、入力装置２０４、表示部２０５、ＬＡＮコントローラ２０６ａが、バスなどの通信線(バス

という）２０７ａに接続することで形成されている。

【００３２】

図１にて示したオブジェクト１１２や、サブジェクト情報１１３、ポリシー情報１２０は、上記外部記憶装置２０３ａに格納され、必要に応じて主記憶２０２ａの領域に読み出して利用される。

【００３３】

また、上記サブジェクト１１１やアクセス制御部１１０は、主記憶２０２ａにロードされ、実行可能プログラムとして上記ＣＰＵ２０１ａによって処理されるものである。特にアクセス制御部１１０は、オペレーティングシステム（ＯＳ）の一部、あるいはＯＳに組み込み可能なプログラムとして処理される。

【００３４】

同様に、上記ポリシー設定支援ツール１００も、主記憶２０２ａにロードされ、上記ＣＰＵ２０１ａによって処理されるものである。

【００３５】

また、ポリシー設定支援ツール１００のうち、ユーザインタフェース部１０１は、上記表示部２０５にユーザインタフェースを表示し、入力装置２０４を介して入力されるデータやコマンドに応じて各種処理を実行する。

【００３６】

また、インストール情報１０５や、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８については、外部記憶装置２０３ａに格納しておき、必要に応じて主記憶２０２ａの領域に読み出して利用してもよい。

【００３７】

ここまでは、情報処理装置２００にて利用されるポリシー情報１２０を、上記ポリシー設定支援ツール１００により設定および更新するために必要なシステム構成である。

【００３８】

次に、例えば入力装置２０４や表示部２０５をもたないサーバ２１０におけるポリシー設定および更新処理を、上記情報処理装置２００から行うためのシステム構成について説明する。

【００３９】

サーバ２１０は、ＣＰＵ２０１ｂ、主記憶２０２ｂ、外部記憶装置２０３ｂの他に、ＬＡＮコントローラ２０６ｂをバス２０７ｂに接続することで形成される。ＬＡＮコントローラ２０６は、主記憶２０２にロードされて実行中のプログラムが、ネットワーク２２０を介して他のネットワークノードとデータを交換するために利用する装置である。

【００４０】

上記アクセス制御部１１０が、サーバ２１０のＯＳあるいはＯＳに組み込み可能なプログラムとして主記憶２０２ｂにロードされてＣＰＵ２０１ｂにより処理され、同じく主記憶２０２ｂにロードされてＣＰＵ２０１ｂにより処理されるプログラムをサブジェクト１１１とみなし、当該サブジェクトからオブジェクト１１２へのアクセスを制御することを前提とし、以下説明する。

【００４１】

なお、ポリシー情報１２０やオブジェクト１１２、サブジェクト情報１１３は、外部記憶装置２０３ｂに格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

【００４２】

このようなシステム構成において、本実施形態のポリシー設定支援ツール１００を利用する場合は、少なくとも入力装置２０４と表示部２０５の利用を前提とする上記ユーザインタフェース部１０１を、情報処理装置２００側の主記憶２０２ａにて実行させ、それ以外のポリシー生成部１０２、アクセス監視部１０３、差分検出部１０４はサーバ２１０側の主記憶２０２ｂにて実行させ、互いにネットワーク２２０を介してデータ交換を行いながら各種処理を実行する。

【００４３】

また、インストール情報１０５や、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８については、外部記憶装置２０３ｂに格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

【００４４】

これにより、遠隔地にある複数のサーバに対しても、同一の情報処理装置からポリシーの設定および更新が可能となる。

【００４５】

図５は、上記ポリシー情報１２０の一例を示したものである。上述のように、本実施形態のポリシー設定支援ツール１００が扱うポリシー情報とは、オブジェクトへアクセス可能なサブジェクトを、プログラム名とユーザ・グループの識別子との組み合わせで指定したものである。

【００４６】

図５の例で言うと、ユーザ名”www”の権限で実行しているプログラム”/as/wserv.exe”のみ、オブジェクト名”/www/pub/*”で示されるファイル群に対してアクセス”R”（読み出し）を許可するといったものである。図５における特徴値とは、プログラムの特徴を表す数値のことであり、例えばプログラムファイルのサイズや、ハッシュ関数を用いて算出した値を利用する。

【００４７】

アクセス発生時に、上記アクセス制御部１１０が特徴値を確認することで、不当に改ざんされたプログラムによるアクセスからオブジェクトを保護することも可能となる。また、図５における時間とは、アクセスを許可する時間帯のことであり、特に指定がない場合は、終日アクセス可能となるよう”00:00－24:00”と設定する。

【００４８】

また、図５におけるソフトウェア名称とは、上記プログラムが構成するソフトウェアに付けられた名称である。これは、利用者がポリシーを編集する際に、ソフトウェア名称を用いてプログラムを指定可能とすることを目的に登録されたものであり、上記アクセス制御部１１０によるアクセス権チェックの際には無視される情報である。

【００４９】

図３は、上記インストール情報１０５や、関連付け情報１０６、サンプル情報１０７、アクセスログ１０８の一例を示したものである。インストール情報１０５とは、上記サブジェクト情報に格納されているプログラムに関する情報を、ソ

フトウェアの種類毎に分類して管理するためのものである。

【００５０】

その内容は、ソフトウェア名称と、実行ファイル名称、当該実行ファイルのインストール先となるディレクトリ名、更には当該ソフトウェアをアンインストールする際に実行すべきアンインストールプログラムの名称といった情報からなる。

【００５１】

図３の例では、”Ｍ３メール3.0”というソフトウェア名称がインストールされており、その実体となる実行ファイルが”M3MAIL.exe”であり、当該実行ファイルのインストール先が”/m3/”ディレクトリの下であり、アンインストールプログラムの名称が”/m3/uninstall.exe”であることを表している。

【００５２】

このような情報は、一般的なオペレーティングシステム（ＯＳ）でも管理している場合が多いことから、本実施形態のポリシー設定支援ツール１００が独自に管理せずに、ＯＳが管理しているインストール情報を利用することも考えられる。

【００５３】

次に、関連付け情報１０６とは、オブジェクト１１２をアクセスする際に、そのアクセス手段として利用される頻度の高いプログラムの情報を、オブジェクトの種類毎に管理するためのものである。図３の例では、ファイル名の拡張子が”txt”のオブジェクトへアクセスする際には、利用者からの特別な指示がない限り、実行ファイル名称が”/tools/gpad.exe”のプログラムを利用することを意味している。

【００５４】

このような情報も、一般的なＯＳが管理している場合が多いことから、本実施形態のポリシー設定支援ツール１００が独自に管理せずに、ＯＳが管理している関連付け情報を利用することも考えられる。

【００５５】

３つ目に、サンプル情報１０７とは、ソフトウェアの種類毎に標準的な、ある

いは推奨のポリシー情報を記述したものである。図３の例では、ソフトウェア名称が”アタッチサーバ2.0”というプログラムを利用するならば、オブジェクト名が”/www/pub/*”で表されるファイルに対しては、実行ファイル名称が”/as/wserv.exe”のプログラムが、ユーザ・グループ名が”www”の権限で実行している場合に限り、アクセスタイプ”R”つまり読み出しのみ許可することを表している。

【００５６】

４つ目に、アクセスログ１０８とは、上記サブジェクト１１１からオブジェクト１１２へのアクセスを、上記アクセス監視部１０３により監視して、当該アクセス内容を記録したものである。図３に示したアクセスログの一行目の例では、オブジェクト名に示されるファイル”/datafile.db”に対して、サブジェクト情報として示されているプログラム名”/db/hdbr.exe”のプログラムがユーザ名”system”の権限によって、アクセスタイプに示されるアクセス”RW”（読み出しと書き込み）を実行したことを表している。

【００５７】

図４は、ポリシー設定支援ツール１００のユーザインタフェース部１０１が、当該ツールの利用者向けに提供するポリシー設定画面４００の一例を示すものである。利用者は、図２の表示部２０５に表示された上記ポリシー設定画面４００を利用することにより、ポリシー情報１２０の設定や更新、参照といった各種編集作業が可能となる。

【００５８】

ポリシー設定画面４００のうち、４１０はポリシー情報１２０に現在登録されているポリシー一覧を表示するボックスである。当該ポリシー表示ボックス４１０は、アクセス対象となるオブジェクト名と、アクセス主体となるサブジェクト情報と、許可されたアクセスタイプと、アクセス可能な時間帯を表す情報から構成される。

【００５９】

図４（ａ）の例では、サブジェクト情報として、ソフトウェアの名称を表示している。これは、図３で示したインストール情報１０５に格納されているソフト

ウェア名称と同じものである。これにより、利用者にとってポリシーの大要を把握し易くなるという効果が期待できる。

【００６０】

４１１は、ポリシーの表示を切り替えるための切替ボタンであり、利用者が当該切替ボタン４１１ａを押下すると、図４（ｂ）に示すように、サブジェクト情報の表示が、プログラム名とプログラムファイルの特徴値、およびユーザ・グループ名といった、より詳細なものへと切り替わる。反対に、図４（ｂ）の切替ボタン４１１ｂを押下すると、図４（ａ）の４１０ａのような、ソフトウェア名称だけの表示へと切り替わる。

【００６１】

このようなサブジェクト情報の表示切り替えを可能とするためには、上記図３に示したインストール情報１０５に格納されたソフトウェア名称を、図５に示すようにポリシー情報１２０に対しても識別子として登録し、各プログラムとソフトウェア名称の対応関係を保持しておけばよい。

【００６２】

または、上記ソフトウェア名称の代わりに、ユニークな識別番号を各ソフトウェアに対して割り当てて、上記インストール情報１０５と上記ポリシー情報１２０の両方に登録してもよい。

【００６３】

また、複数のプログラムファイルから構成されるソフトウェアであれば、それらプログラムファイルには全て同一の識別番号あるいは識別子を、上記ポリシー情報１２０に登録する。多くの場合、それらプログラムファイルの格納先は共通のディレクトリ下であることから、共通のディレクトリ下にあるプログラムファイルに対して同一のソフトウェア識別番号あるいは識別子を割り当てればよい。

【００６４】

上記ユーザインタフェース部１０１は、上記切替ボタン４１１が押下される度に、ポリシー情報１２０を参照しながら上記ポリシー表示ボックス４１０内のサブジェクト情報の表示内容を切り替えることになる。

【００６５】

４２０は、ポリシーを生成、変更するための編集用ボックスである。４２１は、編集用ボックス４２０に記述したポリシーを上記ポリシー表示ボックス４１０に追加して、ポリシー情報１２０に保存するための追加ボタンである。

【００６６】

上記編集用ボックス４２０には、オブジェクト名とサブジェクト情報、アクセスタイプ、時間を指定できるが、これら項目を利用者が一つ一つ入力してもよいし、後述するように簡易設定ボタン４３０を利用して指定することもできる。

【００６７】

また、上記ポリシー表示ボックス４１０からポリシーを選択すると、上記ユーザインタフェース部１０１が、当該ポリシーを上記編集用ボックス４２０に表示するので、既に登録済みのポリシーを一部変更する際には、上記ポリシー表示ボックス４１０に表示されたポリシーから変更したいものを選択して上記編集用ボックス４２０に表示し、必要な修正を加えてから上記追加ボタン４２１を押下すればよい。

【００６８】

上記ポリシー設定画面４００には、上記簡易設定ボタン４３０の他、サンプル登録ボタン４３１、更新ボタン４３２、削除ボタン４３３、終了ボタン４３４がある。以下、これらボタンの意味について説明する。

【００６９】

簡易設定ボタン４３０は、上記サンプル情報１０７や、関連付け情報１０６、アクセスログ１０８等を利用して、ポリシー原案を自動生成する際に押下するボタンである。当該処理については後述する。

【００７０】

サンプル登録ボタン４３１は、上記編集用ボックス４２０の表示内容を上記サンプル情報１０７に登録し、以後サンプルポリシーとして再利用可能なものとする際に押下するボタンである。

【００７１】

更新ボタン４３２は、上記ポリシー情報１２０に登録されているポリシーを、最新のオブジェクトやサブジェクト情報１１３に合わせて更新する際に押下する

ボタンである。この処理についても後述する。

【００７２】

登録済みのポリシーを一部削除したい場合には、上記ポリシー表示ボックス４１０に表示されたポリシーから削除したいものを選択して、削除ボタン４３３を押下する。また、ポリシー編集作業を終了する場合には、終了ボタン４３４を押下する。

【００７３】

図６は、上記簡易設定ボタン４３０を押下したときに、図２の表示部２０５に出現する簡易設定インタフェースの一例を示したものである。利用者は、簡易設定インタフェース６００を通じて、上記サンプル情報１０７を利用したポリシー原案作成や、上記関連付け情報１０６を利用したポリシー原案作成、更には上記アクセスログ１０８を利用したポリシー原案作成を実行することができる。

【００７４】

図６の６０１は、インストールされているソフトウェア一覧表示ボックスであり、上記ユーザインタフェース部１０１が、上記インストール情報１０５およびサンプル情報１０７を参照して、現在インストールされていて且つサンプルポリシーが用意されているソフトウェアのみを表示する。

【００７５】

利用者が、これらソフトウェアのサンプルポリシーを利用してポリシーの原案を作成する場合には、各ソフトウェアに対応したチェックボックス６０３ａにチェックを付けて、原案作成ボタン６０８を押下すればよい。

【００７６】

図６の６０２は、特定のソフトウェアとの関連付けがされているファイル拡張子一覧表示ボックスであり、上記ユーザインタフェース部１０１が上記関連付け情報１０６を参照して表示する。当該関連付け情報を利用してポリシーの原案を作成する場合には、各拡張子に対応したチェックボックス６０３ｂにチェックを付けて、原案作成ボタン６０８を押下すればよい。

【００７７】

図６の６０５は、監視したいプログラムを指定するための入力ボックスであり

、ここにプログラム名を入力して開始ボタン６０６を押下すると、上記アクセス監視部によるアクセス監視と上記アクセスログ１０８への記録を開始する。終了ボタンを押下すると、上記アクセス監視とアクセスログ記録を終了する。

【００７８】

その後で、上記原案作成ボタン６０８を押下すると、アクセスログ１０８を利用してポリシー原案を作成することができる。なお、上記プログラムの指定は、プログラムファイル名の代わりに、ソフトウェアの名称で指定できるものでもよい。

【００７９】

上記のように作成されたポリシー原案は、上記ユーザインタフェース部１０１の処理により、図４の編集用ボックス４２０に表示される。当該ポリシー原案をベースに、利用者が一部修正を加えるなど、編集作業を行ってから上記追加ボタン４２１を押下すると、当該編集されたポリシーを上記ポリシー表示ボックス４１０に追加すると共に、ポリシー情報１２０にも保存する。

【００８０】

図６の６０９は、キャンセルボタンであり、上記簡易設定インタフェース６００の処理を終了して、図４のポリシー設定画面４００へ戻る際に押下する。

【００８１】

図７は、サンプル情報からポリシー原案を生成する処理手順の一例を示したものである。ステップ７０１は、上記ユーザインタフェース部１０１へのコマンド入力であり、これは図６のソフトウェア一覧表示ボックス６０１からソフトウェアを選択して、上記原案作成ボタン６０８を押下することに相当する。

【００８２】

ステップ７０２では、上記ポリシー生成部１０２により、上記選択されたソフトウェアに対応するサンプル情報を取得する。ステップ７０３では、上記差分検出部１０３により、上記サブジェクト情報１１３やオブジェクト１１２を参照して、上記サンプル情報との差分データを作成する。

【００８３】

これは、ソフトウェアのインストール先や、ディレクトリ構成が標準と異なる

場合、上記サンプル情報がそのまま利用できないことがあるためである。ステップ７０４では、上記ポリシー生成部１０２により、上記サンプル情報と差分データを基に、対象となる情報処理装置やサーバに相応しいポリシーの原案を生成する。

【００８４】

このとき、アクセス許可されるプログラムの特徴値算出も併せて行う。また、アクセス許可する時間帯については、特に指定がない限り、終日（00:00－24:00）に設定しておく。ステップ７０５では、上記ユーザインタフェース部１０１により、上記ポリシーの原案を、上記図４の編集用ボックス４２０に表示する。

【００８５】

ステップ７０６では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ７０７では、上記修正後のポリシーを、上記ポリシー情報１２０へ保存する。このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。

【００８６】

次に図８を用いて、関連付け情報１０６を利用したポリシー生成の処理手順の一例を説明する。ステップ８０１は、上記ユーザインタフェース部１０１へのコマンド入力であり、これは図６のファイル拡張子一覧表示ボックス６０２から拡張子を選択して、上記原案作成ボタン６０８を押下することに相当する。

【００８７】

ステップ８０２では、上記関連付け情報１０６を参照して、上記利用者が選択した拡張子に関連付けられたプログラムの実行ファイル名称を取得する。ステップ８０３では、上記ポリシー生成部１０２により、上記取得した情報を基にポリシーの原案を生成する。

【００８８】

このとき生成されるポリシーの原案は、オブジェクト名と、プログラム名と、プログラムの特徴値と、時間帯のみ指定されており、ユーザ・グループ名やアク

セスタイプは指定していない。ただし、図２に示した上記情報処理装置２００やサーバ２１０が利用しているＯＳ自身が、上記アクセス制御部１１０とは異なる独自のアクセス制御機構を備えている場合はその通りでない。

【００８９】

つまり、当該ＯＳ独自のアクセス制御機構があれば、各オブジェクトへのアクセス条件として、ユーザ・グループの情報や、アクセスタイプが設定されているはずである。そこで、例えば上記ポリシー生成部１０２がこれらユーザ・グループの識別子やアクセスタイプを取得して、上記ポリシーの原案に取り込むものであってもよい。

【００９０】

また、同じ拡張子をもつファイルでも、これらユーザ・グループやアクセスタイプが異なるものは、オブジェクト名を区別してそれぞれ個別のポリシーとなるよう原案を作成する。

【００９１】

このようにして生成したポリシー原案は、ステップ８０４にて上記ユーザインタフェース部１０１が、上記図４の編集用ボックス４２０に表示する。ステップ８０５では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

【００９２】

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ８０６では、上記修正後のポリシーを、上記ポリシー情報１２０へ保存する。

【００９３】

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報１０５より取得する。

【００９４】

次に図９を用いて、上記アクセスログ１０８を利用したポリシー生成処理手順の一例を説明する。ステップ９０１は、上記ユーザインタフェース部１０１への

コマンド入力であり、これは図６の入力ボックス６０５にプログラムを指定して、上記開始ボタン６０６を押下することに相当する。

【００９５】

ステップ９０２では、上記アクセス監視部１０３により、上記指定されたプログラムから発行されるファイルアクセスを監視して、その内容を上記アクセスログ１０８に記録する。この処理は、上記図６の終了ボタン６０７を押下するまで継続する。

【００９６】

ステップ９０３では、上記ポリシー生成部１０２により、上記アクセスログ１０８からポリシー原案を生成する。このとき、上記アクセスログ１０８に記録されたアクセスは、正当なアクセスとして許可されるようにポリシー原案を作成する。

【００９７】

また、サブジェクトとなるプログラムの特徴値も算出し、上記ポリシー原案に取り入れる。時間帯指定については、特に指定がない限り”00:00－24:00”（終日）とする。

【００９８】

このようにして生成したポリシー原案は、ステップ９０４にて上記ユーザインタフェース部１０１が、上記図４の編集用ボックス４２０に表示する。ステップ９０５では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

【００９９】

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ９０６では、上記修正後のポリシーを、上記ポリシー情報１２０へ保存する。

【０１００】

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名の他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報１０５より取得する。

【０１０１】

以上の図７から図９の処理を、利用者が必要に応じて繰り返したり、組み合わせたりしながらポリシーを作成することになる。

【０１０２】

次に、図１０を用いて上記差分検出部１０４の処理手順について説明する。これは、上記オブジェクト１１２やサブジェクト情報１１３に変更が生じた場合にも、登録済みのポリシー情報１２０への反映を容易にするための処理である。

【０１０３】

ステップ１００１は、例えば上記ユーザインタフェース部１０１へのコマンド入力であり、これは上記図４の更新ボタン４３２を押下することに相当する。あるいは、図２の上記情報処理装置２００やサーバ２１０に搭載されたＯＳが備えるスケジューラ機能等により、差分検出部１０４の処理を定期的に実行させるものであってもよい。

【０１０４】

そして差分が検出された場合には、ポリシーの記述を見直す必要があることを、上記ユーザインタフェース部１０１を通じて利用者に通知することで、無効なポリシーの記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

【０１０５】

ステップ１００２では、差分検出部１０４が上記ポリシー情報１２０を参照し、当該ポリシー情報１２０に登録されているオブジェクト名とサブジェクト情報を取得する。ステップ１００３では、オブジェクトとサブジェクトに関する最新情報を、上記オブジェクト１１２とサブジェクト情報１１３とから取得し、上記ポリシー情報１２０の内容と照合する。

【０１０６】

ステップ１００４では、上記照合処理の結果、更新の必要があると思われるポリシーについてはその内容を上記ユーザインタフェース部１０１に渡し、図１１に示すように、上記編集用ボックス４２０に表示する。このとき、変更のあった部分が他よりも目立つよう強調表示する。

【０１０７】

利用者は、当該変更内容を目視で確認し（ステップ１００５）、更新しても問題ないと判断するならば、必要な修正を加えた上で、図１１の更新ボタン４２２を押下することで、正式に上記ポリシー情報１２０の内容を更新できる（ステップ１００６）。仮に、プログラムのアップデートをした覚えがないのに、プログラムの特徴値に変更があった場合は、プログラムファイルの不当な改ざんが発生した可能性もあると考えられ、この場合は、利用者はポリシーの更新をせずに上記プログラムファイル改ざんの原因を確認すればよい。

【０１０８】

以上述べたように、本実施形態によれば、ソフトウェアの仕様を詳しく知らなくても、ソフトウェアの種類毎に用意したサンプルポリシーや、関連づけ情報、ソフトウェアのアクセスログを利用することで、適切なポリシーを短時間に作成することができる。

【０１０９】

また、オブジェクトやサブジェクトの情報に変更があった場合でも、変更すべきポリシーの部分が利用者にとって容易に判るよう表示でき、且つ簡易な操作で更新可能であることから、常に適切なポリシー情報に基づくアクセス制御が可能となる。

【０１１０】

【発明の効果】

本発明によれば、ポリシーの作成および維持に要する作業負荷を軽減することが可能になる。

【図面の簡単な説明】

【図１】　本実施形態におけるポリシー設定支援ツールの一構成例を示す図。

【図２】　ポリシー設定支援ツールを利用するためのコンピュータシステムの一構成例を示す図。

【図３】　インストール情報と関連付け情報とサンプル情報とアクセスログの一例を示す図。

【図４】　本実施形態において、ポリシー設定画面４００の一例を示す図。

【図５】　本実施形態において、ポリシー情報１２０の一例を示す図。

【図６】　本実施形態において、簡易設定インタフェース６００の一例を示す図。

【図７】　サンプル情報１０７からポリシーを作成する処理のフローチャートを示す図。

【図８】　関連付け情報１０６からポリシーを作成する処理のフローチャートを示す図。

【図９】　アクセスログ１０８からポリシーを作成する処理のフローチャートを示す図。

【図１０】　差分検出部１０４によるポリシー更新処理のフローチャートを示す図。

【図１１】　編集用ボックス４２０に表示するポリシーの変更情報の一例を示す図。

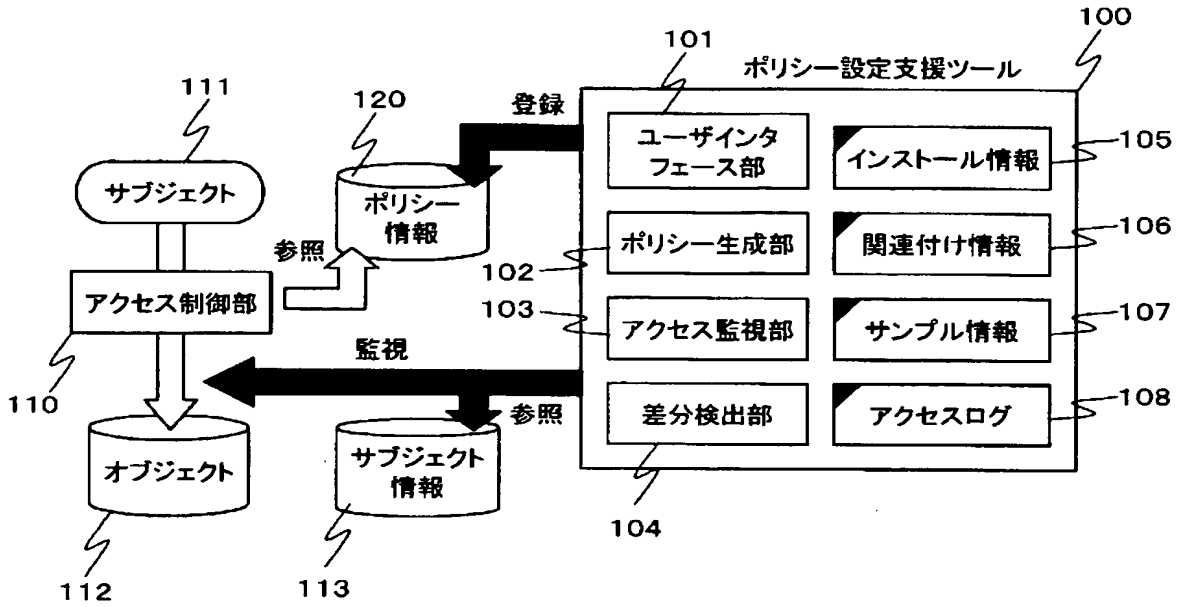
【符号の説明】

１００･･･ポリシー設定支援ツール、１０１･･･ユーザインタフェース部、１０２･･･ポリシー生成部、１０３･･･アクセス監視部、１０４･･･差分検出部、１０５･･･インストール情報、１０６･･･関連付け情報、１０７･･･サンプル情報、１０８･･･アクセスログ、１１０･･･アクセス制御部、１１１･･･サブジェクト、１１２･･･オブジェクト、１１３･･･サブジェクト情報、１２０･･･ポリシー情報、２００･･･情報処理装置、２０１･･･ＣＰＵ、２０２･･･主記憶、２０３･･･外部記憶装置、２０４･･･入力装置、２０５･･･表示部、２０６･･･ＬＡＮコントローラ、２１０･･･サーバ、２２０･･･ネットワーク、４００･･･ポリシー設定画面、４１０･･･ポリシー表示ボックス、４１１･･･切替ボタン、４２０･･･編集用ボックス、４２１･･･追加ボタン、４２２･･･更新ボタン、４３０･･･簡易設定ボタン、４３１･･･サンプル登録ボタン、４３２･･･更新ボタン、４３３･･･削除ボタン、４３４･･･終了ボタン、６００･･･簡易設定インタフェース、６０１･･･ソフトウェア一覧表示ボックス、６０２･･･ファイル拡張子一覧表示ボックス、６０３･･･チェックボックス、６０５･･･入力ボックス、６０６･･･開始ボタン、６０７･･･終了ボタン、６０８･･･原案作成ボタン、６０９･･･キャンセルボタン。

【書類名】図面

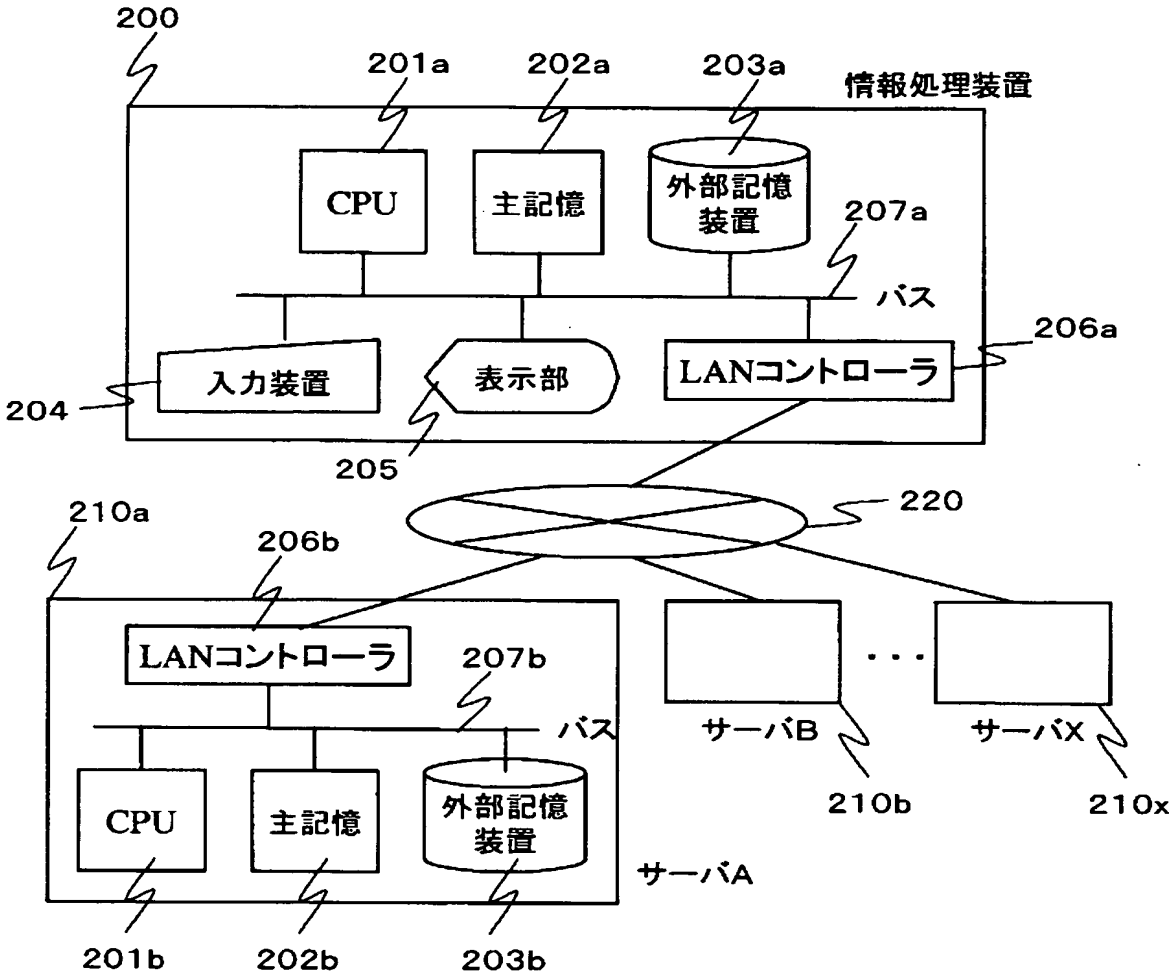
【図１】

図１


100
101
ポリシー設定支援ツール
111
120
登録
サブジェクト
ポリシー情報
ユーザインタフェース部
インストール情報
105
参照
ポリシー生成部
関連付け情報
106
102
アクセス制御部
103
アクセス監視部
サンプル情報
107
監視
110
参照
差分検出部
アクセスログ
108
オブジェクト
サブジェクト情報
104
112
113

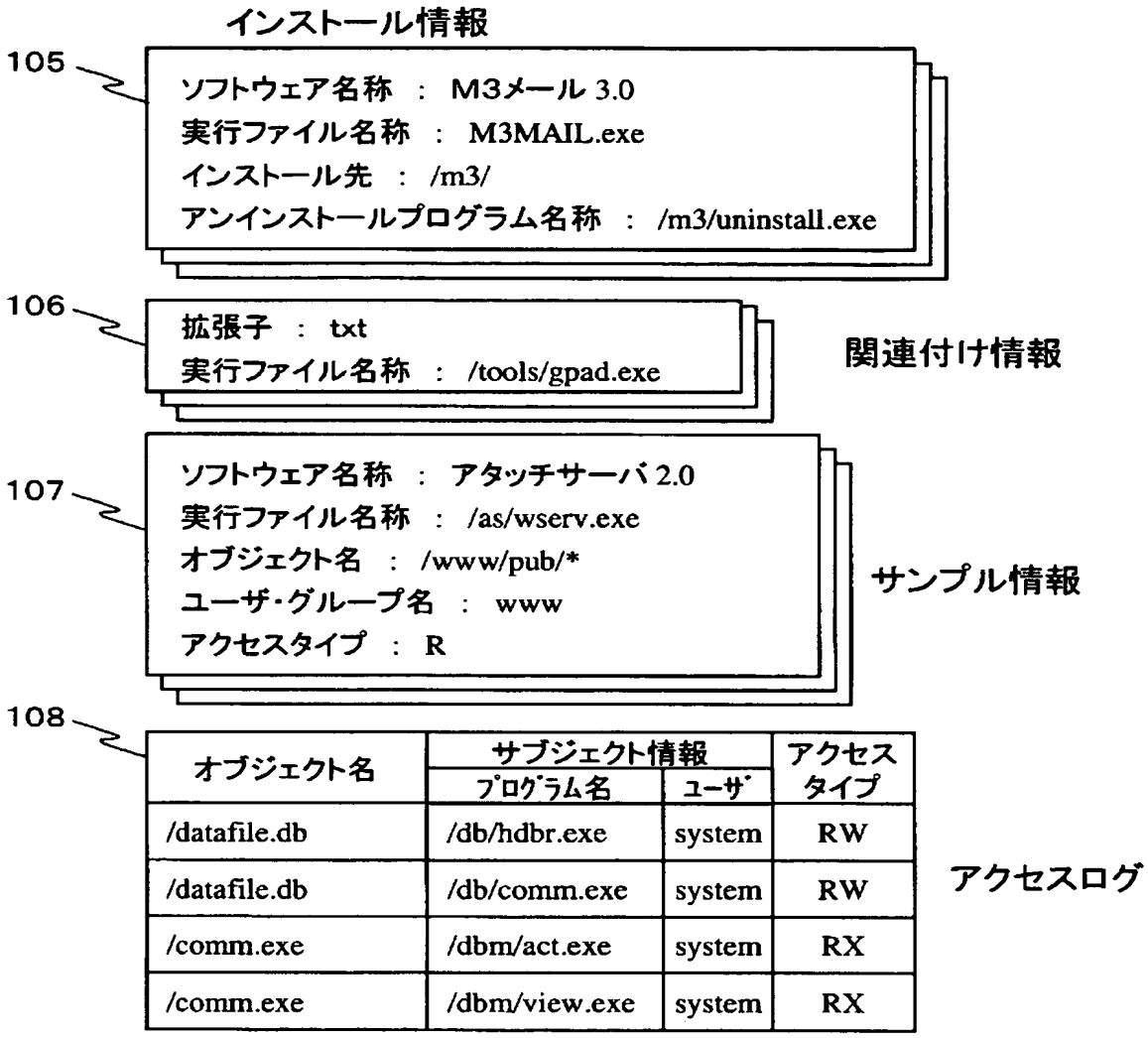
【図２】

図２


200
201a
202a
203a
情報処理装置
CPU
主記憶
外部記憶装置
207a
バス
206a
入力装置
表示部
LANコントローラ
204
205
220
210a
206b
LANコントローラ
207b
バス
CPU
主記憶
外部記憶装置
サーバA
サーバB
サーバX
210b
210x
201b
202b
203b

【図３】

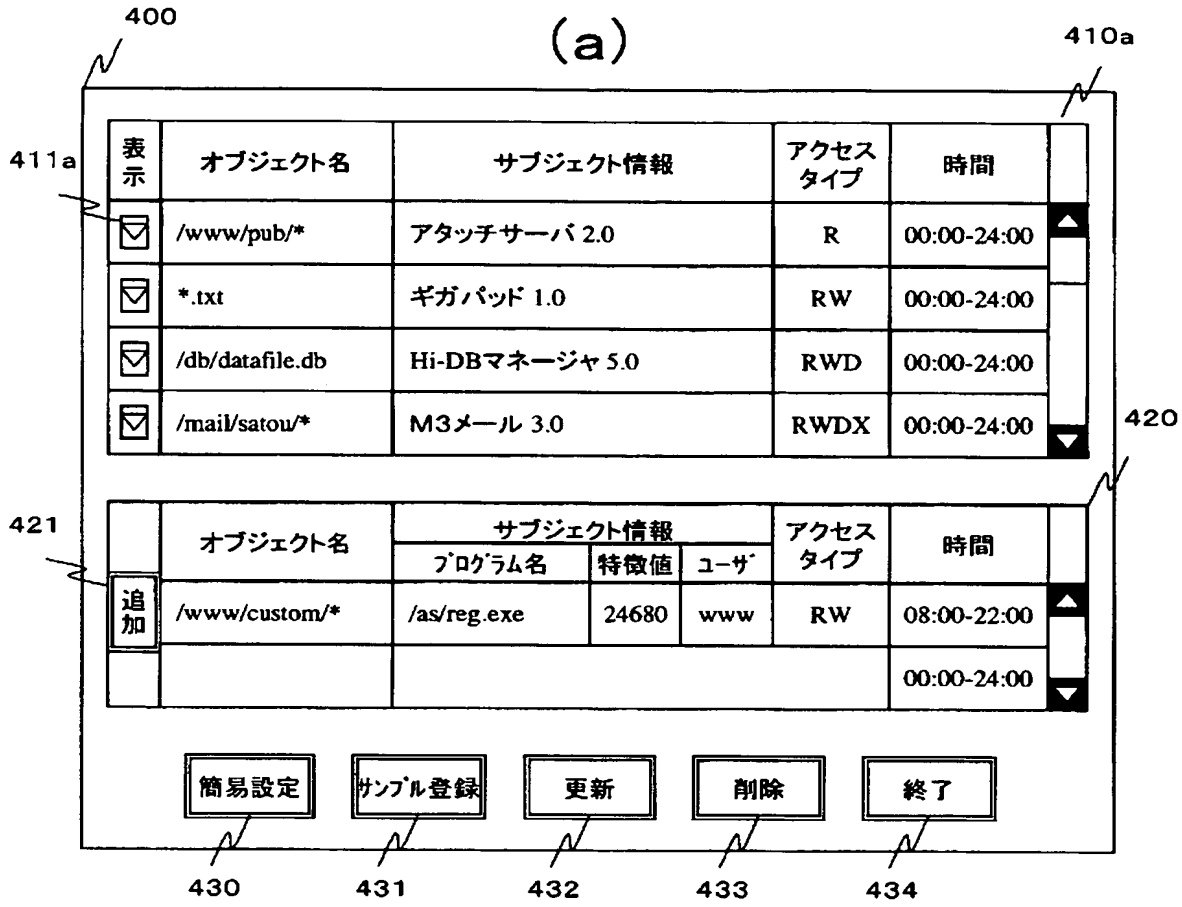
図３

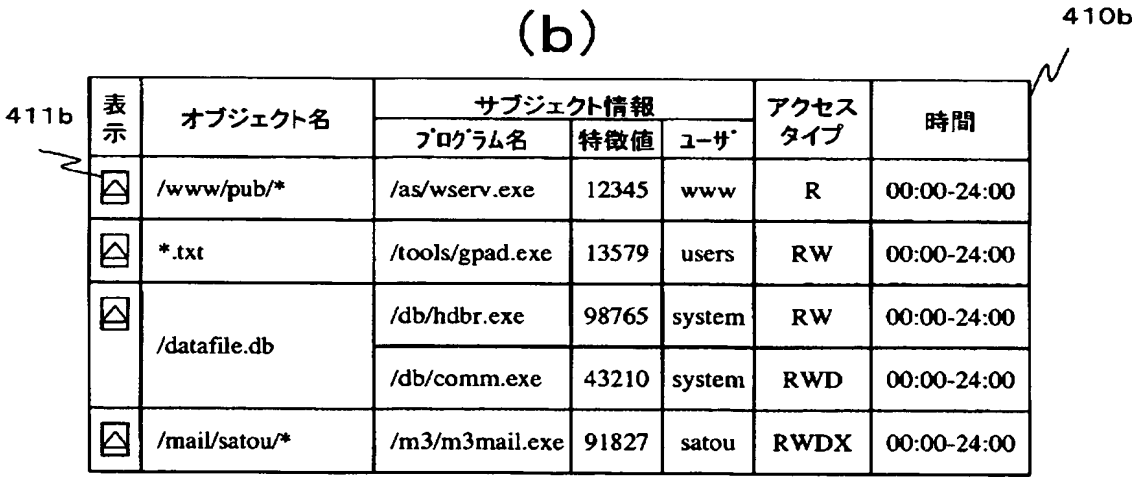


オブジェクト名	サブジェクト情報		アクセスタイプ
	プログラム名	ユーザ	
/datafile.db	/db/hdbr.exe	system	RW
/datafile.db	/db/comm.exe	system	RW
/comm.exe	/dbm/act.exe	system	RX
/comm.exe	/dbm/view.exe	system	RX

【図４】

図４


400
(a)
410a
411a
表示
オブジェクト名
サブジェクト情報
アクセスタイプ
時間
/www/pub/*
アタッチサーバ 2.0
R
00:00-24:00
*.txt
ギガパッド 1.0
RW
00:00-24:00
/db/datafile.db
Hi-DBマネージャ 5.0
RWD
00:00-24:00
/mail/satou/*
M3メール 3.0
RWDX
00:00-24:00
420
421
オブジェクト名
サブジェクト情報
プログラム名
特徴値
ユーザ
アクセスタイプ
時間
追加
/www/custom/*
/as/reg.exe
24680
www
RW
08:00-22:00
00:00-24:00
簡易設定
サンプル登録
更新
削除
終了
430
431
432
433
434


(b)
410b
411b
表示
オブジェクト名
サブジェクト情報
プログラム名
特徴値
ユーザ
アクセスタイプ
時間
/www/pub/*
/as/wserv.exe
12345
www
R
00:00-24:00
*.txt
/tools/gpad.exe
13579
users
RW
00:00-24:00
/datafile.db
/db/hdbr.exe
98765
system
RW
00:00-24:00
/db/comm.exe
43210
system
RWD
00:00-24:00
/mail/satou/*
/m3/m3mail.exe
91827
satou
RWDX
00:00-24:00

【図５】

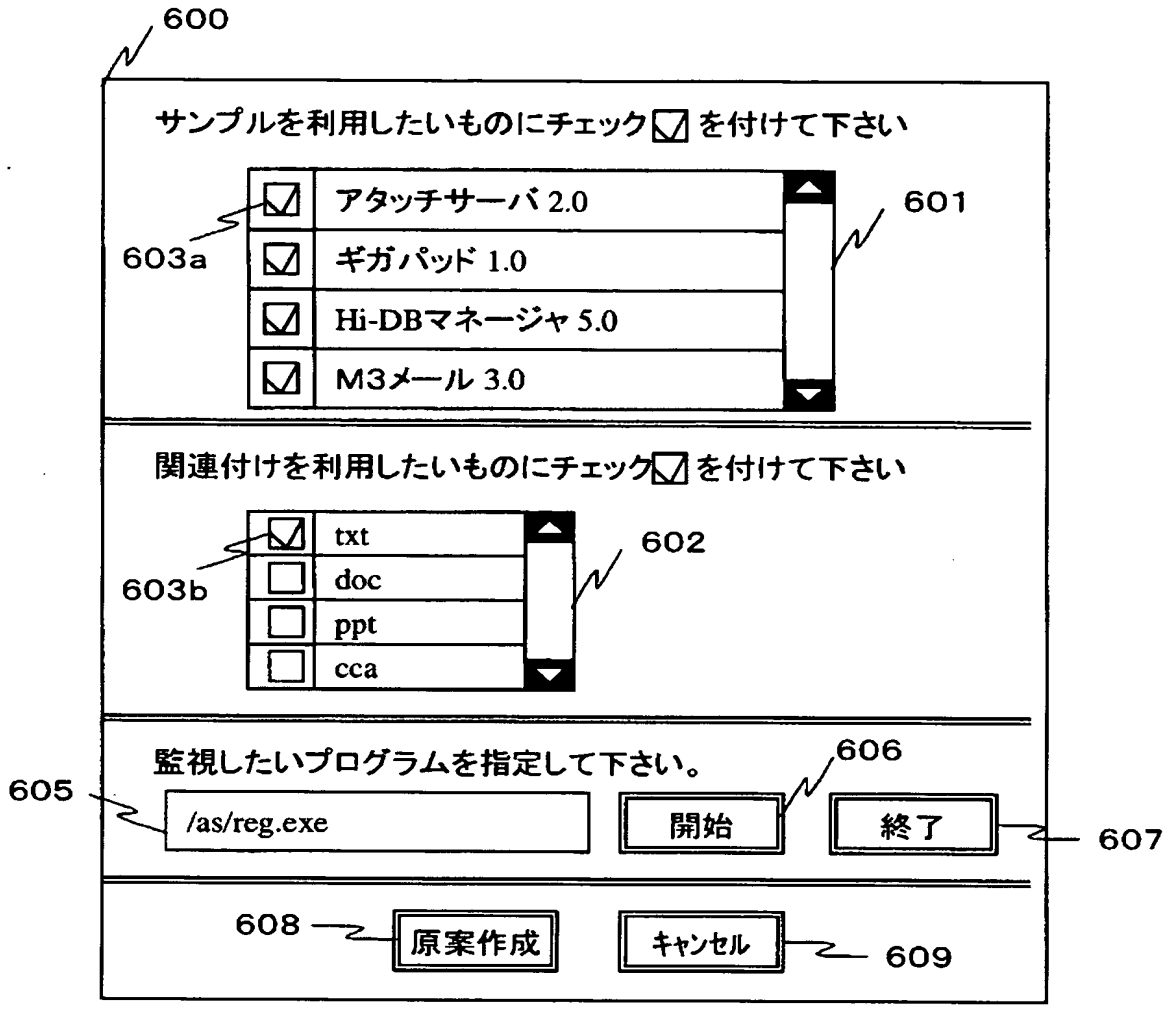
図５

120

オブジェクト名	サブジェクト情報				アクセスタイプ	時間
	ﾌﾟﾛｸﾞﾗﾑ名	特徴値	ﾕｰｻﾞ	ソフトウェア名称		
/www/pub/*	/as/wserv.exe	12345	www	アタッチサーバ2.0	R	00:00-24:00
*.txt	/tools/gpad.exe	13579	users	ギガパッド1.0	RW	00:00-24:00
/datafile.db	/db/hdbr.exe	98765	system	Hi-DBマネージャ5.0	RW	00:00-24:00
	/db/comm.exe	43210	system	Hi-DBマネージャ5.0	RWD	00:00-24:00
/mail/satou/*	/m3/m3mail.exe	91827	satou	M3メール3.0	RWDX	00:00-24:00

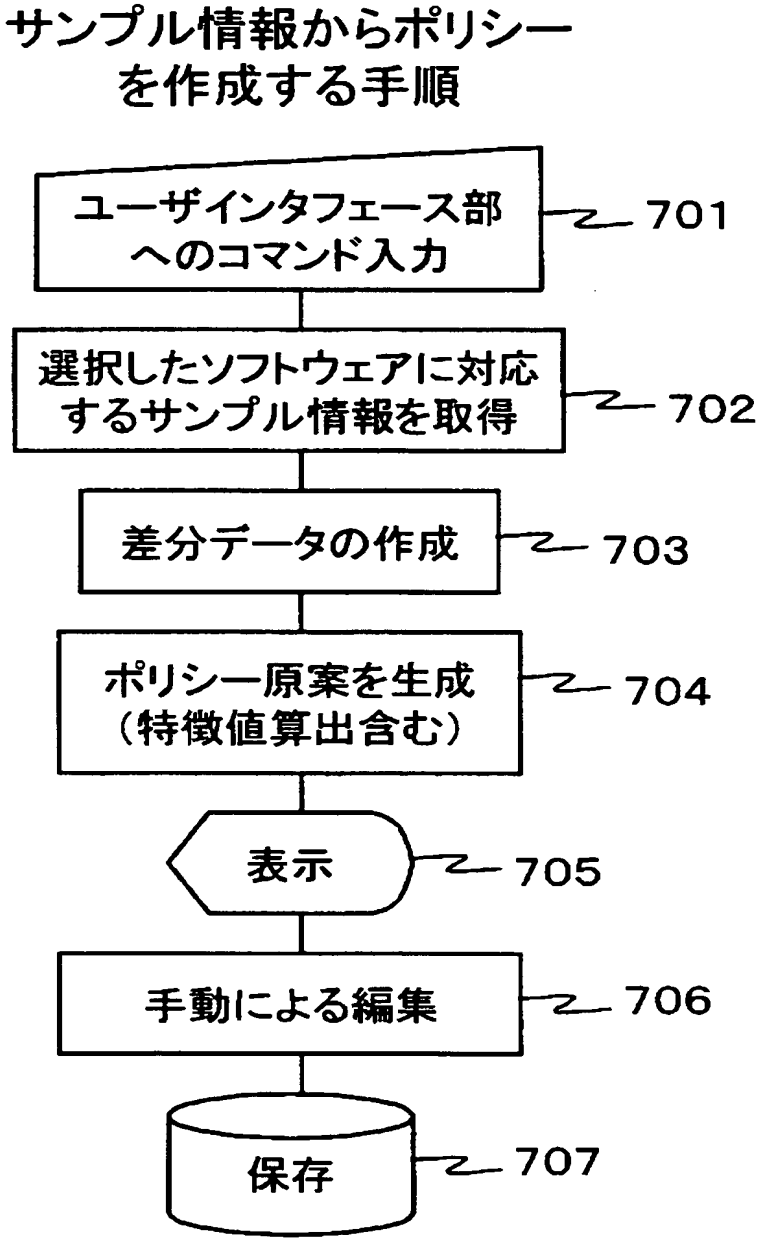
【図６】

図６


600
サンプルを利用したいものにチェック☑を付けて下さい
603a
アタッチサーバ 2.0
ギガパッド 1.0
Hi-DBマネージャ 5.0
M3メール 3.0
601
関連付けを利用したいものにチェック☑を付けて下さい
603b
txt
doc
ppt
cca
602
監視したいプログラムを指定して下さい。
605
/as/reg.exe
606
開始
終了
607
608
原案作成
キャンセル
609

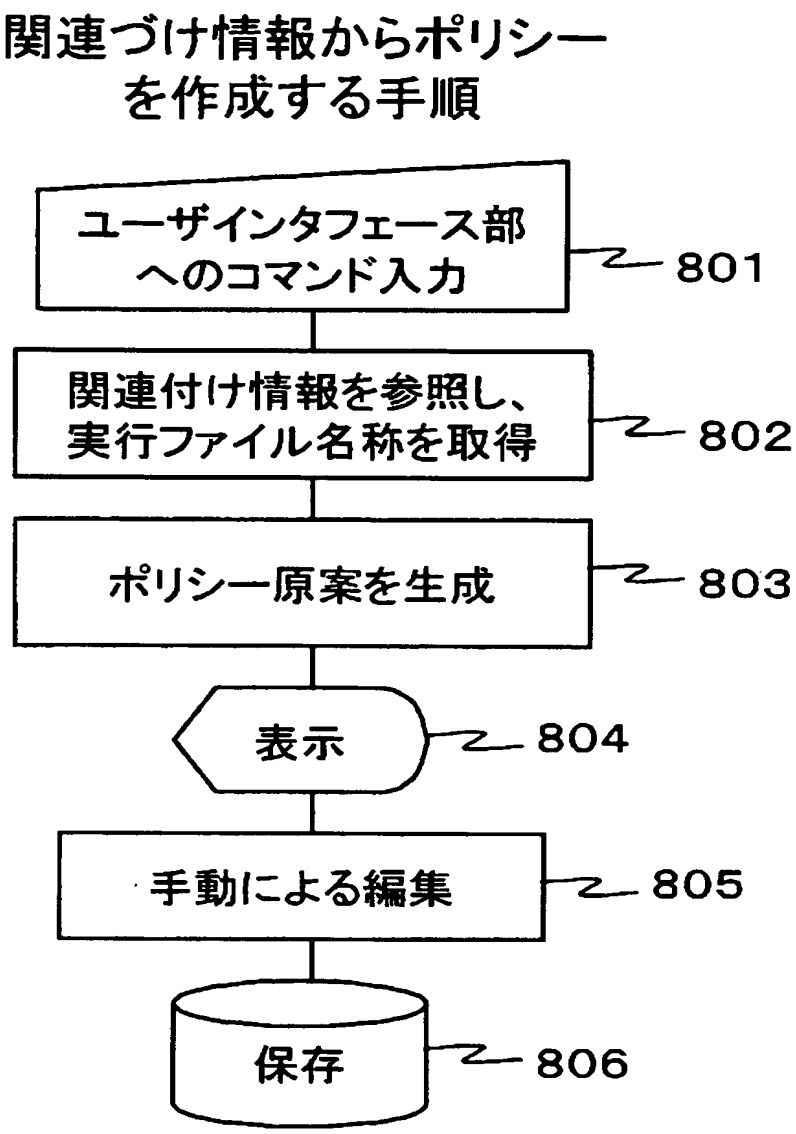
【図７】

図７


サンプル情報からポリシー
を作成する手順
ユーザインタフェース部
へのコマンド入力
701
選択したソフトウェアに対応
するサンプル情報を取得
702
差分データの作成
703
ポリシー原案を生成
（特徴値算出含む）
704
表示
705
手動による編集
706
保存
707

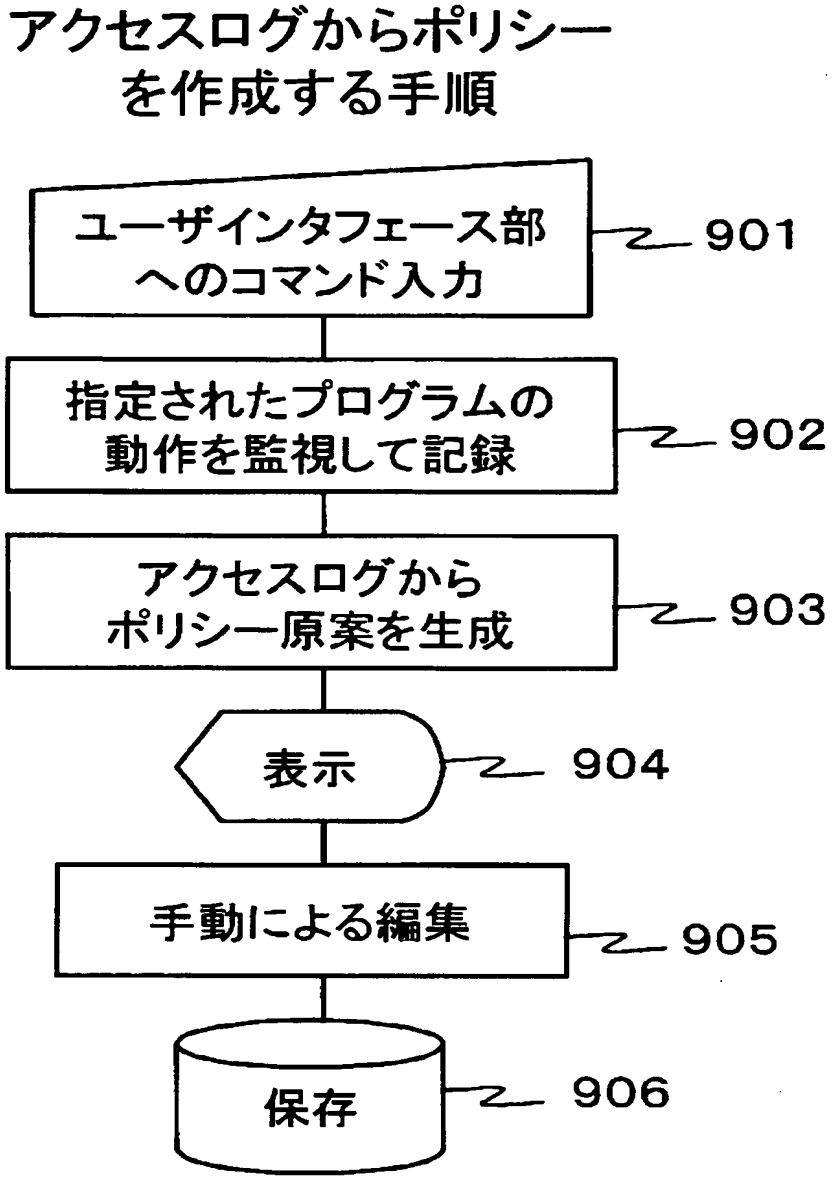
【図８】

図８


関連づけ情報からポリシー
を作成する手順
ユーザインタフェース部
へのコマンド入力
801
関連付け情報を参照し、
実行ファイル名称を取得
802
ポリシー原案を生成
803
表示
804
手動による編集
805
保存
806

【図９】

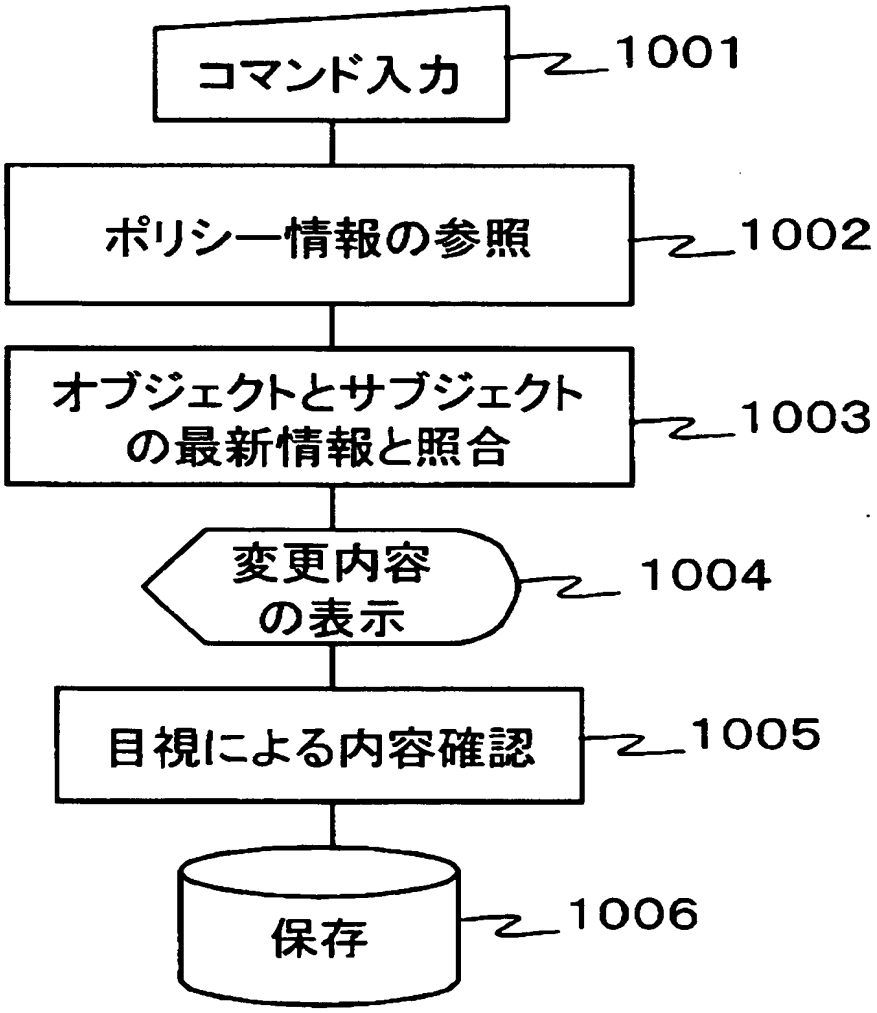
図９


アクセスログからポリシー
を作成する手順
ユーザインタフェース部
へのコマンド入力
901
指定されたプログラムの
動作を監視して記録
902
アクセスログから
ポリシー原案を生成
903
表示
904
手動による編集
905
保存
906

【図１０】

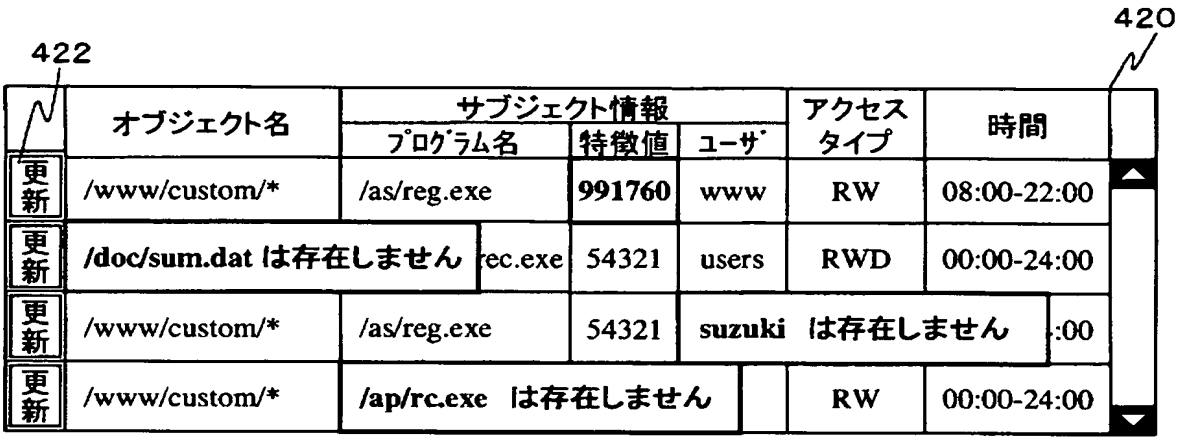
図１０

差分検出部の処理



【図１１】

図１１


420
422
オブジェクト名
サブジェクト情報
プログラム名
特徴値
ユーザ
アクセスタイプ
時間
更新
/www/custom/*
/as/reg.exe
991760
www
RW
08:00-22:00
更新
/doc/sum.dat は存在しません
ec.exe
54321
users
RWD
00:00-24:00
更新
/www/custom/*
/as/reg.exe
54321
suzuki は存在しません
:00
更新
/www/custom/*
/ap/rc.exe は存在しません
RW
00:00-24:00

【書類名】要約書

【要約】

【課題】アクセス制御ポリシーの設定を、各ソフトウェアの仕様を知らなくても適切に設定、且つ維持可能なポリシー設定支援ツールを提供する。

【解決手段】ソフトウェアの種類毎のポリシーを記述したサンプル情報と、オブジェクトの種類毎に利用頻度の高いプログラムの情報を記述した関連付け情報と、プログラムの動作を監視して記録したアクセスログ情報のいずれかを用いてポリシーの原案を作成するポリシー生成部１０２と、ポリシー原案を表示して、利用者による確認と編集を可能とするユーザインタフェース部１０１の処理により、適切なポリシー設定に必要な作業の簡易化を実現する。また差分検出部１０４により、設定済みポリシーから更新すべき部分を、現在のオブジェクト１１２とサブジェクト情報１１３を参照して検出し、ユーザインタフェース部１０１を通じて提示するとともに、簡易に更新可能とすることで、適切なポリシー維持も可能とする。

【選択図】図１

認定・付加情報

特許出願の番号	特願２００２－３０２４３９
受付番号	５０２０１５５９７１１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年１０月１８日

＜認定情報・付加情報＞

【提出日】　平成14年10月17日

次頁無

特願２００２－３０２４３９

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所